

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE USE OF A
DEVICE TO COLLECT INFORMATION
ABOUT A TARGET COMPUTER
CONNECTING TO THE WIRELESS
ROUTER BELONGING TO BIBLE
BAPTIST CHURCH, NASHUA, NEW
HAMPSHIRE

Case No. 1:20-mj- 113-01-AJ

Filed Under Seal – Level II

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Shawn Serra, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 to authorize law enforcement to employ an electronic investigative technique further described in Attachment B, in order to identify a computer or other device capable of accessing the internet (the “Target Computer”) used to possess, receive, and distribute child pornography by connecting to the wireless router with Service Set Identifier (“SSID”)¹ BBCN, located at the Bible Baptist Church, 62 Caldwell Rd., Nashua, New Hampshire.

2. I have been employed as an HSI Special Agent since June of 2005, and am currently assigned to the Manchester, New Hampshire Resident Office. I graduated from the University of Massachusetts, Lowell, Massachusetts with a Bachelor of Science Degree in

¹ An SSID is the name of a wireless network, typically chosen by the person who sets up the network.

Criminal Justice. In 2003, I graduated from the University of Massachusetts, Lowell, Massachusetts with a Master of Arts Degree in Criminal Justice. I have also received training in the areas of child sexual exploitation including violations pertaining to possession and production of child pornography by attending a twenty-three-week training program at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. As part of my duties, I have observed and reviewed examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, to include digital/computer media. During the course of this investigation, I have also conferred with other investigators who specialize in computer forensics and who have conducted numerous investigations which involved child sexual exploitation offenses. I completed the Basic Computer Evidence Recovery Training (“BCERT”) in September 2018 and I am A+ certified, an entry level certification in information technology.²

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. While I have included all of the material information relevant to the requested warrant, it does not set forth all of my knowledge about this matter.

² In drafting this warrant, I have consulted with Nashua Police Detective Peter LaRoche who has specialized knowledge of the Device investigators intend to use. Detective LaRoche is a Detective with the Nashua Police Department (NPD) and has been a full time certified Police Officer in the State of New Hampshire since March 2003. Detective LaRoche is currently assigned to the Computer Forensics Unit (CFU) within the Criminal Investigations Division (CID). Detective LaRoche has been assigned to this unit since February 2017. Detective LaRoche has advanced training computer forensics investigations, computer networking, networks intrusion investigations, malware analysis, and he holds multiple certifications in computer forensics. Detective LaRoche has received this training from the United States Secret Service, National Computer Forensic Institute, and Homeland Security Investigations. Prior to his assignment in CFU, Detective LaRoche worked in the Patrol Division within the Uniform Field Operations Bureau.

4. This Court has authority to issue the requested warrant under Federal Rule of Criminal Procedure Rule 41(b)(1) & (2) because the Target Computer is believed to be located inside this district because it has connected to a wireless router located in Nashua, New Hampshire on various dates beginning in 2017, and as recently as February 2020.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252(a)(2), relating to the possession, receipt and distribution of child pornography, have been committed, are being committed, and will be committed by the person using the Target Computer. There is also probable cause to believe that the identifying information of the Target Computer will constitute evidence of those criminal violations. In addition, in order to obtain additional evidence relating to the Target Computer, its user, and the criminal violations under investigation, law enforcement must first identify the Target Computer. There is probable cause to believe that the use of the investigative technique described by the warrant will result in officers learning that identifying information.

6. Because collecting the information authorized by this warrant may fall within the statutory definitions of a “pen register” or a “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), this warrant is designed to comply with the Pen Register Statute as well as Rule 41. *See* 18 U.S.C. §§ 3121-3127. This warrant therefore includes all the information required to be included in a pen register order. *See* 18 U.S.C. § 3123(b)(1). The investigative technique discussed herein is relevant to HSI's ongoing investigation of the distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2)

PROBABLE CAUSE

7. On August 10, 2016, the National Center for Missing and Exploited Children (“NCMEC”) sent the Nashua Police Department (“NPD”) fourteen “Cybertips” submitted by Skype. According to the Cybertips, user “paigekatrinahemmis” with email address paigekatrinahemmis@yahoo.com had uploaded fourteen images of child pornography on July 12, 2016, between the hours of 1:51:45 p.m. and 1:52:55 p.m.³ from the IP address 73.218.175.5.⁴ The IP address from which the images were uploaded was subscribed to the Bible Baptist Church, located at 62 Caldwell Road, Nashua, New Hampshire at that date and time.

8. An April 4, 2017, NCMEC sent the NPD a Cybertip submitted by Google. According to the Cybertip, Google user “Ray Comfort” with associated email addresses massage4unh@gmail.com and jillianlepka@yahoo.com had uploaded four images of child pornography. Google did not provide the exact date and time the uploads occurred but provided the date and time of the registration of the account, November 24, 2016, at 12:16:06 a.m., and two dates and times of logins to the account, January 5, 2017, at 3:49:27 p.m. and 3:50:05 p.m. The Cybertip also provided the IP addresses for the registration and logins which was 2603:3005:3400:3700:b1c0:2300:af44:1b2e. At those dates and times, the IP address was subscribed to the Bible Baptist Church, located at 62 Caldwell Road, Nashua, New Hampshire.

³ Most of the times discussed in this affidavit were originally provided in UTC but investigators converted them to EDT/EST for ease of reference.

⁴ “**Child Pornography**”, as used herein, is defined in Title 18 United States Code § 2256 (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

9. On May 2, 2017, NCMEC sent three additional Cybertips to the NPD, reported by Skype. According to those Cybertips, on April 30, 2017 between 11:42:56 p.m. and 11:50:58 p.m., Skype user live:kaitj_3 uploaded three images of child pornography from IP address 75.67.41.17. At that date and time, the IP address was subscribed to the Bible Baptist Church, located at 62 Caldwell Road, Nashua, New Hampshire.

10. In June of 2017, NPD detectives drove to the area of the Bible Baptist Church and conducted a survey of Wi-Fi signals in the area during which time they observed a locked Wi-Fi signal titled “BBCN.” This abbreviation is believed to stand for “Bible Baptist Church of Nashua.” I know that a “locked” Wi-Fi signal requires a password to access it.

11. In October of 2017, NPD and HSI spoke with the pastor of the Bible Baptist Church, Stephen Bates who advised that the church offers free Wi-Fi under the name “BBCN” to its members which is password protected. According to Bates, however, the password is “123456” and is widely known throughout the congregation. Pastor Bates could not identify any potential suspects and advised that the church is typically always unlocked. Pastor Bates said that he maintains his own wireless network at his residence on the church property.

12. In January 2019, I received a referral from Special Agent Robert Andrews, who is assigned to the HSI Field Office in Denver, Colorado. SA Andrews was conducting an online child sexual exploitation investigation targeting individuals producing and distributing surreptitiously-recorded child pornography through the Onion Router (Tor) network⁵ and

⁵ Tor was originally designed, implemented, and deployed as a project of the U.S. Naval Research Laboratory for the primary purpose of protecting government communications. It is now part of the public domain and is maintained and updated by The Tor Project, a 501(c)(3) non-profit organization located in Seattle, WA. The Tor Project defines the Tor network as “a group of volunteer-operated servers that allows people to improve their privacy and security on

Instagram. Through their investigation, SA Andrews and other law enforcement officers identified a Colorado residence used to produce some of the child pornography and obtained a federal search warrant for that residence. Law enforcement officers seized several electronic devices during execution of the search warrant. Through forensic analysis of the seized electronic devices and interviews of the suspect (hereinafter referred to as “Target A”) and victims, law enforcement officers identified several Instagram and email accounts used to disseminate child pornography videos.

13. Target A has been identified as a male resident of Colorado with two children. Investigators have identified one of Target A’s daughters as Minor Victim 1 through a distinctive mark on her body. They confirmed that Target A was involved in the production and distribution of child pornography involving Minor Victim 1.

14. Among other things, SA Andrews later obtained and executed a federal search warrant for an Instagram account in the name “Samantha_brinn” (hereinafter referred to as “Instagram Account 1”), which was used to discuss the production and distribution of child pornography with Target A. Pursuant to the warrant, Instagram provided Instagram Account 1’s full account activity, including the content of direct messages and IP addresses, for the period of April 12, 2016, through November 11, 2018. The data provided by Instagram confirmed that the user of Instagram Account 1 shared child pornography with others, including Target A, other

the Internet...by connecting (users) through a series of virtual tunnels rather than making a direct connection.” Furthermore, “Tor’s onion services let users publish websites and other services without needing to reveal the location of the site.” In order to access the Tor network, a user must install the software either by downloading it into the user’s existing web browser, downloading The Tor Project’s free web browser with the software already embedded, or downloading a publicly-available third-party application. Using the Tor network prevents someone attempting to monitor an Internet connection from learning what sites a user visits and prevents the sites the user visits from learning the user’s physical location. Because of the way the Tor network routes communication through randomly selected and unrelated computers on the network, traditional IP address identification techniques are not viable.

child pornography collectors, and minor victims. For example, on August 21, 2018 at 10:37 p.m., the user of Instagram Account 1 distributed a nude image of a female on her knees with a focus on her anus and genitals during a direct message exchange. SA Andrews recognized the bedroom and the female's ring as those belonging to Minor Victim 1 identified during his investigation. As this photo was discussed on December 24, 2015, the oldest Minor Victim 1 could be at that time would be 15. Accordingly, I believe that Minor Victim 1 was approximately 15 years old when this sexually explicit image was taken. As the user of Instagram Account 1 also communicated with Minor Victim 1's father, I believe the image likely came from him.

15. Instagram identified the IP address used by Instagram Account 1 during the August 22, 2018 direct message as 24.61.89.176. Using an online IP lookup tool, SA Andrews determined that IP address 24.61.89.176 was registered to Comcast. SA Andrews sent an administrative summons to Comcast, and learned that IP address 24.61.89.176 was assigned to Bible Baptist Church, with service address 117 Fairview Ave. OFC, Nashua, NH, and billing address 62 Caldwell Road, Nashua, NH, for the relevant period.

16. The person using Instagram Account 1 also discussed having a sexual relationship with a female with the initials L.B. when L.B. was between her junior and senior years in high school. The user sent clothed photographs of L.B. over the internet. I confirmed that L.B. is a person who lives in Raymond, New Hampshire, and is affiliated with the BBCN.

17. Over multiple direct message sessions, the user of Instagram Account 1 urged Target A to obtain an account with Google so that they may continue their child exploitation activities, including distribution of child pornography. Instagram Account 1 provided Target A with the google email address Kooldot3 to continue their conversations. In April 2019, agents

received a warrant to search kooldot3@gmail.com. The warrant showed that the account was closed and provided no content or information about the account other than the dates it was open and closed (June 12, 2017 through February 7, 2018).

18. A forensic exam of Target A's Macbook located Yahoo Instant Messenger (YIM) chat history for user "dnd0100." In a chat occurring on December 25, 2015, at 3:47 p.m., YIM user dnd0100 and YIM user "jillianlepka" discuss YIM user dnd0100 obtaining naked photos of Minor Victim 1, and therefore I believe dnd0100 to be Target A. During this chat, YIM user dnd0100 told YIM user jillianlepka that he has a video of Minor Victim 1 sending sexually explicit photos on Snapchat, including "a pussy shot from behind!" I note that jillianlepka is similar to the email address associated with the April 2017 Cybertip I received. The Denver investigators issued a subpoena for the jillianlepka YIM account. Login IDs affiliated with that account included samantha_lep and lorna_themagnificent@yahoo. I note that "lorna" is the first name of L.B. Additionally, the full name listed was "Its me Again."

19. In June of 2019 members of NPD and HSI again spoke with Pastor Bates who consented to a search of the one computer within the church. During the search, nothing of evidentiary interest was located. Pastor Bates provided names of people affiliated with the church in positions such as information technology, security, and online advertisement but this information did not produce any investigative leads.

20. In late March of 2020, the NPD was contacted by the Tallahassee, Florida Police Department because a child sexual abuse victim had observed sexually explicit photographs of herself taken when she was a child on the website MEGA.nz. Detectives in Tallahassee obtained information for the MEGA account posting the pictures, l_blairm@protonmail.com, and

observed three IP addresses associated with activity sessions on September 26, 2019 at 11:54 a.m., February 14, 2020 at 12:17 p.m., and February 25, 2020 at 5:12 p.m.. The IP addresses were: 2603:3005:3400:7800:34f6:6317:722d:c2b1 (September 26, 2019); 2603:3005:3400:7800:81d9:7359:fc62:90d1 (February 14, 2020); and 2603:3005:3400:7800:3183:2fca:1efd:bb59 (February 25, 2020). All three IP addresses resolved back to the Bible Baptist Church in Nashua, New Hampshire. This email address is also consistent with the full name of L.B. Additionally, there was a large amount of child pornography located on the MEGA account which used the email address. Detectives in Tallahassee served legal process to proton mail which did not help identify a suspect as the company did not retain any identifying information about the person who created the account.

21. Through conducting research on Comcast Cable Communications I know that Comcast assigns all internet customers dynamic IP addresses, meaning the IP address is assigned by the network each time the user connects and can change over time. Business-class internet customers have the option of obtaining static IP addresses, meaning the IP address does not change for the time period of the service. Through my experience in reviewing Comcast's response to summonses, I know that they will identify if the account is dynamically assigned (dynamic IP address) or statically assigned (static IP address). From 2016 to February of 2020, the account belonging to the Bible Baptist Church has been dynamically assigned, that is, unless a service change is made, the IP address will change over time as users connect. Importantly, the dynamic IP address does not affect or change the SSID.

22. On April 6, 2020, Detective Rayho conducted surveillance of the Bible Baptist Church, during which time, using his cell phone, he observed the network titled “BBCN” to be active and locked.

23. Based on the facts set forth in this affidavit, there is probable cause to believe that a person who has access to the church wireless router with SSID BBCN has distributed child pornography in violation of 18, U.S.C. § 2252(a)(2). There is probable cause to believe that the same person has accessed this wireless network to download child pornography as at least two of the tips received by law enforcement involved a similar login of “jillianlepka” and others relate to the name of L.B.

24. I believe that use of the device described herein will provide evidence of these violations by helping to identify the person using the Target Computer.

MANNER OF EXECUTION

25. In my training and experience, and based on conversations I have had with others trained in these techniques, I have learned that Wi-Fi is a family of wireless networking technologies which are commonly used for local area networking of devices and Internet access. Devices that can use Wi-Fi technologies include desktop and laptop computers, smartphones and tablets, smart TVs, printers, digital audio players, digital cameras, cars and drones, among other things. Wi-Fi uses radio waves that allow a device (laptop, phone, etc.) to communicate with something such as a router. That wireless router then converts the radio waves back into data and then sends that data to the Internet using a physical connection. To get data from the Internet, the process is reversed.

26. When any two machines communicate with each other, they need certain standards and protocols defined to enable them to communicate. IEEE 802.11 refers to the set of standards that define communication for wireless local area networks. IEEE stands for Institute of Electrical and Electronics Engineers.

27. A media access control address (“MAC address”) is a unique identifier assigned to a network interface controller (NIC) attached to or installed in a device (computer, laptop, cell phone, router, etc.) for use as a network address in communications within a network. That is, every device which connects to the internet has a unique MAC address which is assigned by the device manufacturer.⁶ This use is common in most IEEE 802 networking technologies, including Ethernet, Wi-Fi, and Bluetooth. As typically represented, MAC addresses are recognizable as six groups of two hexadecimal digits, separated by hyphens, colons, or without a separator (ex. D4:61:9D:A6:FE:11). MAC addresses are primarily assigned by device manufacturers and are therefore often referred to as the burned-in address, Ethernet hardware address, hardware address, or *physical address*. Every device which connects to the internet has a unique MAC address which is assigned by the device manufacture.

28. An organizationally unique identifier (OUI) is a 24-bit number that uniquely identifies a vendor or manufacturer. They are purchased and assigned by the IEEE. The OUI is the first three octets of a MAC address. For example, D4:61:9D would tell me that a certain devices is owned by Apple, Inc. A Base Service Set Identifier (BSSID) is the MAC address for a wireless access point such as a router.

⁶ The user of the device does have the ability to change the MAC address originally assigned by the manufacturer.

29. As previously mentioned, a Service Set Identifier (SSID) is the generally readable and customizable name assigned by owner of the wireless access point like a router (i.e. “Home”). In this case, the SSID of the wireless access point at the Bible Baptist Church of Nashua is “BBCN.”

30. Whenever Wi-Fi on a device is turned on it openly broadcasts the SSIDs (network names) of all previously associated networks in an attempt to connect to one of them. These small packets, called probe requests, are publicly viewable by anyone in the area running simple, free, and openly available software run on almost any consumer computer. Probe requests include the unique device fingerprint called a MAC address that can be used to specifically identify each device. Many of the times these probe requests are broadcast as an identifiable network name history (names like “Bob’s Home,” “Bob’s Work,” “Starbucks,” etc.).

31. Smart phones are constantly scanning for beacon frames broadcast by wireless access points and using the phone’s GPS to associate those network’s MAC addresses with the phone’s location.

32. It is possible by passively monitoring the public broadcasts made by Wi-Fi access points as well as the MAC addresses, SSIDs, and probes of devices connected to and in the area of the access points, to develop a possible identity of the owner/user(s) of both the access points and connected devices. Wi-Fi capable devices and access points constantly publicly broadcast this information. This method of public Wi-Fi monitoring does not intercept, reroute, decrypt, modify, or otherwise intrude upon the contents of private network traffic.

33. To facilitate the execution of this warrant, law enforcement will use an investigative device or devices, methodologies and techniques, to collect several possible types of electronic information regarding devices connected to the target wireless network, BBCN. The information collected may include Media Access Control (MAC) Address(s), wireless signal strength, Wifi management frame information publicly broadcast by wireless devices including beacons,⁷ probe requests⁸ and responses,⁹ associations, disassociations,¹⁰ authentications, and de-authentications.¹¹

⁷ Beacons: Are a periodic advertisement broadcast out to tell any listening devices that this SSID is available and has particular features / capabilities. Client devices depend upon these beacon frames to discover what networks are available, and to ensure that the networks that they are associated with are actually still present and available.

⁸ Probe Requests: A probe request is a special frame sent by a client station requesting information from either a specific access point, specified by SSID, or all access points in the area, specified with the broadcast SSID. The information being requested in a probe includes the supported data rates, which are also included in the beacon frames typically broadcast from an access point. By sending a probe request your wireless card is making an active scan of either a specific network or all networks in the area.

⁹ Probe Response: Typically when an access point hears a probe request frame, either directed at the specific access point or to all stations in the area using the broadcast SSID, it will send out a probe response. Similar to a beacon frame, probe responses contain much of the same information required for two stations to begin communicating.

¹⁰ Association: In the client association process, access points send out beacons announcing one or more SSIDs, data rates, and other information. The client sends out a probe and scans all the channels and listens for beacons and responses to the probes from the access points. The client associates to the access point that has the strongest signal. If the signal becomes low, the client repeats the scan to associate with another access point. During association, the SSID, MAC address, and security settings are sent from the client to the access point and checked by the access point.

¹¹ Authentication: Is the first step in network attachment. Authentication requires a mobile device (station) to establish its identity with an Access Point (AP) or broadband wireless router. No data encryption or security is available at this stage. (basically when you do the password if its required)

AUTHORIZATION REQUEST

34. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41. The proposed warrant also will function as a pen register order under 18 U.S.C. § 3123.

35. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days from the end of the period of authorized surveillance. This delay is justified because there is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the operator of the subject wireless router would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). There is reasonable necessity for the use of the technique described above, for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

36. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to identify those who connect to the subject wireless router outside of daytime hours for 30 days or until the Target Computer is identified, whichever ends first.


37. A search warrant may not be legally necessary to compel the investigative technique described herein. Nevertheless, I hereby submit this warrant application out of an abundance of caution.

Respectfully submitted,

/s/ Shawn Serra
Shawn Serra, Special Agent
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Dated: June 9, 2020



ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE



ATTACHMENT A

This warrant authorizes the use of the electronic investigative technique described in Attachment B to collect data from the wireless access device with SSID BBCN, located at the Bible Baptist Church of Nashua, 62 Caldwell Rd., Nashua, New Hampshire, and from devices that connect to that wireless router.

ATTACHMENT B

This warrant authorizes the officers to whom it is directed to use the device discussed herein to collect several possible types of electronic information regarding devices connected to the target wireless network, BBCN. The information collected may include Media Access Control (MAC) Address(s), wireless signal strength, Wifi management frame information publicly broadcast by wireless devices including beacons, probe requests and responses, associations, disassociations, authentications, and de-authentications and the network and/or device name of the device connecting to the wireless network, from all internet capable devices that connect to the subject wireless router (identified by the SSID BBCN). The device may be used at any hour of the day or night for 30 days or until the Target Computer is identified. Investigators seek to identify the Target Computer which has used the wireless network at issue to distribute, receive and possess child pornography in violation of 18 U.S.C. § 2252(a)(2). If investigators ascertain the identity of the Target Computer before 30 days, they will end the collection.

Although the Device may recognize other wireless devices that send beacons and/or probes to the wireless network with SSID BBCN, I will only collect data from Devices that connect to the wireless network.

This warrant does not authorize the interception of any telephone calls, text messages, or other electronic communications, and this warrant prohibits the seizure of any tangible property. The Court finds reasonable necessity for the use of the technique authorized above. *See* 18 U.S.C. § 3103a(b)(2).